EXHIBIT J

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT AND SOCIAL SECURITY NUMBERS

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

Washington, DC

June 15, 2004

I. INTRODUCTION

Mr. Chairman, and members of the Subcommittee, I am J. Howard Beales, III, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on identity theft and Social Security numbers. The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. Through this testimony, the Commission will describe the results of a recent survey on the prevalence and impact of identity theft, the ways in which Social Security numbers are collected and used, new protections for consumers and identity theft victims, and the Commission's identity theft program.

II. UNDERSTANDING THE IMPACT OF IDENTITY THEFT

On November 1, 1999, the Commission began collecting identity theft complaints from consumers in its national database, the Identity Theft Data Clearinghouse (the "Clearinghouse").[2] Every year since has seen an increase in complaints.[3] The Clearinghouse now contains over 600,000 identity theft complaints taken from victims across the country. By itself, though, these self-reported data do not currently allow the FTC to draw any firm conclusions about the incidence of identity theft in the general population. To address this important issue, the FTC

---

[1]The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

[2]*See infra* Section V for a discussion of the Commission's mandate to maintain an identity theft complaint database pursuant to the 1998 Identity Theft Assumption and Deterrence Act.

[3] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

commissioned a survey last year to gain a better picture of the incidence of identity theft and the impact of the crime on its victims.[4] The results were startling. The data showed that within the 12 months preceding the survey, 3.23 million persons discovered that an identity thief opened new accounts in their names. An additional 6.6 million consumers learned of the misuse of an existing account. Overall, nearly 10 million people – or 4.6 percent of the adult population – discovered that they were victims of some form of identity theft. These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to individual victims, and almost 300 million hours spent by victims trying to resolve their problems.

Moreover, identity theft is a growing crime. The survey indicated a significant increase in the previous 2-3 years - - nearly a doubling from one year to the next, although the research showed that this increase has recently slowed. Notably, this recent increase primarily involved the misuse of an existing account, which tends to cause less economic injury to victims and is generally easier for them to identify and fix. Overall, the 2003 survey analysis puts the incidence rates of identity theft into sharper focus, and demonstrates the need for a concerted effort between the public and private sectors to act aggressively to reduce identity theft.

III. SOCIAL SECURITY NUMBER USES AND IDENTITY THEFT

Social Security numbers play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Preventing identity thieves from obtaining Social Security numbers will help to protect consumers from this pernicious crime. The potential for misuse arises because Social Security numbers are crucial to

---

[4]The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at http://www.consumer.gov/idtheft/stats.html.

the proper functioning of our financial system. Social Security numbers are used to match consumers to their credit and other financial information. Without them, information may be attributed to the wrong consumer, and the accuracy of credit reports may be degraded. Enabling Social Security numbers to be used appropriately will help to ensure that consumers continue to enjoy the benefits of our current credit system. The Commission is studying "the efficacy of increasing the number of points of identifying information that a credit reporting agency is required to match to ensure that a consumer is the correct individual to whom a consumer report relates before releasing a consumer report to a user" as required by the Fair and Accurate Credit Transactions Act of 2003.[5] This study, to be completed by December, 2004, should greatly increase our knowledge of the importance of Social Security numbers in the matching process. The Commission looks forward to reporting its findings to Congress.

Social Security numbers are collected by public and private entities for various purposes, and several federal and state laws restrict the use or disclosure of Social Security numbers, depending on the source.[6] The nationwide credit bureaus are primary private sources of Social

---

[5]Pub. L. No. 108-396, § 318 (2003).

[6]As GAO has reported, government and commercial entities use social security numbers for a number of different purposes, including to verify the eligibility of applicants, manage records, and conduct research. U.S. General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: Feb 16, 1999) and *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002). As examined in GAO's most recent report of January 2004, information resellers, consumer reporting agencies, and health care organizations obtain social security numbers both directly from consumers and other businesses, and the entities use them for various purposes, including identification and to match the consumer to information stored in the consumer's credit report. *See* U.S. General Accounting Office, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs and Laws Limit the Disclosure of This Information*, GAO-04-11 (Washington, D.C.: Jan. 22, 2004).

Security numbers, collecting information from financial institutions for credit reporting purposes. This information typically includes a consumer's identifying information – such as name, address, and Social Security number – as well as information related to the consumer's credit accounts. The identifying information collected by the credit bureaus is one of the most reliable and comprehensive sources of this information, because individuals tend to provide their financial institutions with accurate and up-to-date identifying information and the credit bureau databases contain information for over 200 million consumers.[7]

The Gramm-Leach-Bliley Act ("GLBA")[8] imposes certain restrictions on the reuse and redisclosure of the identifying information – including Social Security numbers – that is collected by credit bureaus from financial institutions.[9] As a general matter, the GLBA prohibits financial institutions from disclosing nonpublic personal information ("NPI") to nonaffiliated third parties without first providing consumers with notice and the opportunity to opt out of such disclosure. This general restriction, however, is subject to certain exceptions. The information may flow from financial institutions to others for certain purposes specified in the statute and rule,

---

[7] *See* Consumer Data Industry Association's Web site, *available at* http://www.cdiaonline.org/about.cfm.

[8] Subtitle A of Title 5 of the GLBA, 15 U.S.C. §§ 6801-6809.

[9] The GLBA applies to any "nonpublic personal information" ("NPI") that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, Social Security number, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.*, 65 Fed. Reg. 33,646, 33680 (May 24, 2000) (the FTC's Privacy Rule). This identifying information generally is not covered by the Fair Credit Reporting Act. *See FTC v. Trans Union*, Dkt. 9255, Op. of the Commission at pp. 30-31 (Mar. 1, 2000) (holding that consumer name, Social Security number, address, telephone number, and mother's maiden name do not constitute a consumer report under the FCRA).

including, for example, to process transactions or to report consumer information to credit bureaus.[10] When information is disclosed under these GLBA exceptions, the recipient may not use or disclose that NPI except "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."[11]

IV. NEW PROTECTIONS FOR IDENTITY THEFT VICTIMS

On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted.[12] Many of the provisions amend the Fair Credit Reporting Act ("FCRA"),[13] and provide new and important measures to prevent identity theft and facilitate identity theft victims' recovery. Some of these measures will take effect this year.[14] They will codify many of the voluntary measures initiated by the private sector and improve other recovery procedures already in place.

---

[10]These exceptions are found in § 502(e) of the GLBA, and in §§ 313.14 and 313.15 of the FTC's privacy rule. The other GLBA privacy rules contain substantially similar provisions. The § 313.14 exceptions relate to the processing and servicing of transactions at the consumer's request, and the § 313.15 exceptions contain a broad range of unrelated exceptions, such as preventing fraud, assisting law enforcement, complying with subpoenas, and reporting to credit bureaus. Section 313.13 also contains an exception to the notice and opt out requirement, but that section is not relevant here because it relates to contractual arrangements with service providers and joint marketers.

[11]16 C.F.R. 313.11(a)(1)(iii), (c)(3) (2000).

[12]Pub. L. No. 108-396 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

[13]15 U.S.C. § 1681 *et seq.*

[14]The statute set effective dates for certain sections and required the Commission and the Federal Reserve Board jointly to set effective dates for the remaining sections. *See* Effective Dates for the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 602.1 (2004).

One prominent benefit of these amendments to the FCRA is the greater access to free consumer reports.[15] Previously under the FCRA, consumers were entitled to a free consumer report only under limited circumstances.[16] Beginning in December of this year with a regional rollout, nationwide and nationwide specialty consumer reporting agencies[17] must provide free credit reports to consumers once annually, upon request.[18] Free reports will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also enable consumers to detect identity theft early.

Other measures that act to prevent identity theft include:

- *National fraud alert system*:[19] Consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home,[20] can place an alert on their credit files. The alert will put

---

[15]Pub. L. No. 108-396, § 211 (2003).

[16]Previously, free reports were available only pursuant to the FCRA when the consumer suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was on welfare. Absent one of these exceptions, consumers had to pay a statutory "reasonable charge" for a file disclosure; this fee is set each year by the Commission and is currently $9. *See* 15 U.S.C. § 1681j. In addition, a small number of states required the CRAs to provide free annual reports to consumers at their request.

[17]Section 603(w) of the FCRA defines a "nationwide specialty consumer reporting agency" as a consumer reporting agency that compiles and maintains files on consumers relating to medical records or payments, residential or tenant history, check writing history, employment history, or insurance claims, on a nationwide basis. 15 U.S.C. § 1681a(w).

[18]*See* Free Annual File Disclosures, 16 C.F.R. §§ 610.1 and 698.1 (2004).

[19]Pub. L. No. 108-396, § 112 (2003).

[20]The Commission is developing a rule on the duration of this active duty alert. *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23372 (April 28, 2004) (to be

(continued...)

potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the "joint fraud alert" initiative administered by the three major credit reporting agencies. After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each credit reporting agency now shares that request with the other two nationwide credit reporting agencies, thereby eliminating the need for the victim to contact each of the three agencies separately.

- *Truncation of credit and debit card receipts*:[21] In some instances, identity theft results from thieves obtaining access to account numbers on credit card receipts. FACTA seeks to reduce this source of fraud by requiring merchants to truncate the full card number on electronic receipts. The use of truncation technology is becoming widespread, and some card issuers already require merchants to truncate.[22]

- *"Red flag" indicators of identity theft*:[23] The banking regulators and the FTC will jointly develop a rule to identify and maintain a list of "red flag" indicators of identity theft. The goal of this provision is for financial institutions and creditors

---

[20](...continued)
codified at 16 C.F.R. pt. 613).

[21]Pub. L. No. 108-396, § 113 (2003).

[22]FACTA creates a phase-in period to allow for the replacement of existing equipment.

[23]*Id.* § 114.

to analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.

- *Disposal of Consumer Report Information and Records*:[24] The banking regulators and the FTC are coordinating a rulemaking to require proper disposal of consumer information derived from consumer reports.[25] This requirement will help to ensure that sensitive consumer information, including Social Security numbers, is not simply left in a trash dumpster, for instance, once a business no longer needs the information.[26]

FACTA also includes measures that will assist victims with their recovery. These provisions include:

- *Identity theft account blocking*:[27] This provision requires credit reporting agencies immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits an identity theft report,[28] unless there is reason to believe the report is false. Blocking would mitigate the harm to consumers' credit records that can result from identity theft. Credit reporting

---

[24] *Id.* § 216.

[25] Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21388 (April 20, 2004) (to be codified at 16 C.F.R. pt. 682).

[26] In its outreach materials, the FTC also advises consumers to shred any sensitive information before disposing of it.

[27] Pub. L. No. 108-396, § 152 (2003).

[28] The Commission is developing a rule to define the term "identity theft report." *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23371 (April 28, 2004) (to be codified at 16 C.F.R. pt. 603).

agencies must also notify information furnishers who must then cease furnishing the fraudulent information and may not sell, transfer, or place for collection the debt resulting from the identity theft.

- *Information available to victims*:[29] A creditor or other business must give victims copies of applications and business records relating to the theft of their identity at the victim's request. This information can assist victims in proving that they are, in fact, victims. For example, they may be better able to prove that the signature on the application is not their signature.
- *Prevention of re-reporting fraudulent information*:[30] Consumers can provide identity theft reports directly to creditors or other information furnishers to prevent them from continuing to furnish fraudulent information resulting from identity theft to the credit reporting agencies.

When fully implemented, these provisions should help to reduce the incidence of identity theft, and help victims recover when the problem does occur.

---

[29]Pub. L. No. 108-396, § 151 (2003).

[30]*Id.* § 154.

V. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[31] The Identity Theft Act strengthened the criminal laws governing identity theft[32] and focused on consumers as victims.[33] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints, to make available and to refer these complaints to law enforcement for their investigations, and to provide victim assistance and consumer education. Thus, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[34]

---

[31]Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

[32]18 U.S.C. § 1028(a)(7) made identity theft a crime by focusing on the unlawful use of an individual's "means of identification," which broadly includes "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

[33]Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

[34]Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Corporate Marketing Solutions, Inc.*, CIV - 02 1256 PHX RCB (D. Ariz Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards) and *FTC v. C.J.*, CIV - 03 5275 GHK (RZx) (C. D. Cal. July 24, 2003) (final order); *FTC v. Hill*, CV-H-03-5537 (S.D. Tex. Dec. 3, 2003) (final order); and

(continued...)

To fulfill the Act's mandate, the Commission implemented a program that focuses on three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website, (2) maintaining and promoting the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Assisting Identity Theft Victims

The Commission takes complaints from victims through a toll-free hotline, 1-877-ID THEFT (438-4338),[35] and a secure online complaint form on its website, www.consumer.gov/idtheft. In addition, the FTC provides advice on recovery from identity theft. Callers to the hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities.[36] Victims are currently advised to:[37] (1)

---

[34](...continued)

FTC v. M.M., CV-04-2086 (E.D. NY May 18, 2004) (final order) (defendants sent "phishing" spam purporting to come from AOL or Paypal and created look-alike websites to obtain credit card numbers and other financial data from consumers that defendants used for unauthorized online purchases.). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (Jan. 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

[35]The Commission has a separate toll-free line (877-FTC-HELP) to serve those with general consumer protection complaints.

[36]Spanish speaking counselors are available for callers who select the Spanish-language option on the toll-free line.

[37]As the relevant provisions of FACTA become effective, the Commission will update its advice to victims on their new rights and procedures for recovery.

obtain copies of their credit reports from the three national consumer reporting agencies and have a fraud alert placed on their credit reports;[38] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the FCRA,[39] the Fair Credit Billing Act,[40] the Truth in Lending Act,[41] and the Fair Debt Collection Practices Act.[42] If another federal agency can assist victims because the nature of the victims' identity theft falls within such agency's jurisdiction, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form, which allows victims to enter their identity theft information into the Clearinghouse. Victims also immediately can read and download all of the resources necessary

---

[38] These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name.

[39] 15 U.S.C. § 1681 *et seq.*

[40] *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[41] *Id.* § 1601 *et seq.*

[42] *Id.* § 1692 *et seq.*

for reclaiming their credit record and good name, including the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*.[43] The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims and how to correct more intensive credit-related problems that may result from identity theft. It also describes other federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.3 million copies of the booklet since its release in February 2000, and recorded over 1.4 million visits to the Web version.[44]

B. The Identity Theft Data Clearinghouse

One of the primary purposes of the Identity Theft Act was to enable criminal law enforcement agencies to use a single database of victim complaints to support their investigations. To ensure that the database operates as a national clearinghouse for complaints, the FTC accepts complaints from external sources such as other state or federal agencies as well as directly from consumers through its call center and online complaint form. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the

---

[43] *Identity Theft: When Bad Things Happen to Your Good Name* and the secure complaint form are available in Spanish.

[44] Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name*.

prevalence of identity theft complaints by states and by cities.[45] Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse in July of 2000, more than 970 law enforcement agencies, from the federal to the local level, have signed up for secure online access to the database. Individual investigators within those agencies have the ability to access the system from their desktop computers 24 hours a day, seven days a week.

The Commission actively encourages even greater use of the Clearinghouse. Beginning in 2002, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the United States Postal Inspection Service, and the United States Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, seminars have been held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, Phoenix, New York City, Seattle, San Antonio, Orlando, and Raleigh. The FTC also helped the Kansas and Missouri offices of the U.S. Attorney and State Attorney General conduct a training seminar in Kansas City. More than 1500 officers have attended these seminars, representing more than 600 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program.[46] The staff creates preliminary investigative reports by examining significant patterns of identity theft activity in the

---

[45] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

[46] The referral program complements the regular use of the database by all law enforcers from their desktop computers.

Clearinghouse and refining the data through the use of additional investigative resources. Then the staff refers the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers throughout the country for further investigation and potential prosecution. The FTC is aided in this work by its federal law enforcement partners including the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service who provide staff and other resources. Recently, an FBI analyst has worked intensively with the Clearinghouse complaints, using sophisticated analytical software to find related complaints and combine the information with other data sources available to the FBI.

C. Outreach and Education

The Identity Theft Act also directed the FTC to educate consumers about identity theft. Recognizing that law enforcement and private industry each play an important role in helping consumers both to minimize their risk and to recover from identity theft, the FTC expanded its outreach and education mission to include these sectors.

(1) *Consumers*: The FTC has taken the lead in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print and online materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase awareness for the average consumer and provide tips for minimizing the risk of identity theft, the FTC developed a new primer on identity theft, *ID Theft: What's It All*

About?.[47] Taken together with the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the two publications help to educate consumers.

(2) *Law Enforcement*: Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described previously (*see infra* Section V.B), the staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. Other outreach initiatives include: (i) Participation in a "Roll Call" video produced by the Secret Service, which has been sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (ii) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations.

(3) *Industry*: The private sector can help with the problem of identity theft in several ways. From prevention through better security and authentication, to helping victims recover, businesses play a key role in reducing the impact of identity theft.

(a) Information Security Breaches: The FTC works with institutions that maintain personal information to identify ways to help keep that information safe from identity theft.[48] In 2002, the FTC invited representatives from financial institutions, credit

---

[47]Since its release in May 2003, the FTC has distributed almost 554,000 paper copies and over 75,000 web versions, and developed a Spanish version.

[48]The Commission also has law enforcement authority relating to information security. In addition to developing the Disposal Rule pursuant to FACTA, *see supra* Section IV, the (continued...)

issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance.[49] To provide standardized assistance in these types of cases, the FTC developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that is available on the identity theft website. The kit provides advice on contacting consumers, law enforcement agencies, business contact information for the three major credit reporting agencies, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know to protect themselves from identity theft.

(b) Victim Assistance: Identity theft victims may spend substantial time and effort restoring their good names and financial records. As a result, the FTC devotes

---

[48](...continued)
Commission also is responsible for enforcing its GLBA Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. FTC Safeguards Rule, 16 C.F.R. § 314.1 (2002). In brief, the Safeguards Rule requires financial institutions to develop a written information security plan that includes certain elements that are basic to security.

In the past few years, the FTC has also brought enforcement actions against four companies that the Commission alleged made false promises about securing sensitive consumer information, in violation of Section 5 of the FTC Act. 15 U.S.C. § 45(a) These actions resulted in settlements with those companies that collected sensitive information from consumers while making such promises. Those actions arise out of the Commission's finding that these companies' security measures were inadequate and their information security claims therefore were deceptive. *See, e.g., In re Microsoft Corp.*, FTC Dkt. C-4069, Final Decision and Order available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf (Dec. 20, 2002).

[49]*See, e.g.* the incidents involving TriWest (Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12) and Ford/Experian (Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1).

substantial resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[50] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through April 2004, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been nearly 557,000 hits to the Web version. The affidavit is available in both English and Spanish.

VI. CONCLUSION

Identity theft places substantial costs on individuals and businesses. The Commission looks forward to working with businesses on better ways for them to protect the valuable information of consumers with which they are entrusted as well as other means of preventing identity theft. The Commission anticipates that as the new provisions of FACTA take effect, they will further help to reduce identity theft as well as its impact on victims.

---

[50] *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).